FORTRA

GUIDE (FORTRA BRAND PROTECTION)

Navigating Social Media Threats

Social media has revolutionized the way individuals and businesses communicate, swiftly becoming a prime target for threat actors. About 10 years ago, the social media landscape was dominated by giants like Facebook and Twitter. Today, these platforms are just two among many that people use to connect online. With over 5.2 billion users worldwide, social media presents a vast attack surface, making it essential for security teams to understand and mitigate the risks these channels pose to their organizations.

In this guide, we discuss the social media threat landscape size and types, industries that are impacted by these threats, how to turn social media data into intelligence, and mitigation solutions. To successfully protect against threats on social media, security teams should:

1. Understand the different threat types and identify which apply to your organization
2. Create defined criteria to curate intelligence
3. Develop relationships that will lead to effective mitigation

Threat Landscape

Social media is becoming a top online channel for threat actors. Two driving forces behind increased abuse are the ease of account creation and the trust users put in social media. In the last 12 months, 241 million new users subscribed to a social platform. Of those, countless were reported as fake. That means when a user interacts with a post, clicks on a link, or fills out a form, odds are they are unknowingly interacting with a bot.

In order to proactively protect against and remove threats on social media, security teams must be able to identify the attacks on platforms relevant to their organization and understand each specific threat type.

Types Of Social Media Abuse

Cybercriminals employ a wide range of tactics to target organizations on social media. Below are some of the most common and impactful threats to be aware of.

Financial Scams

These threats arise when attackers demand monetary compensation from their victims and are among the most common on social media, often paired with impersonation schemes. Financial scams come in many forms and impact multiple industries across the board.

Types of financial scams include:

Deposit Fraud

Victims are manipulated to deposit fake checks into their accounts and send the threat actor a portion of the money. A victim can become complicit in this type of scam by sending a check to the threat actor for deposit, then reporting it stolen. After the threat actor removes and distributes the cash from the account, the bank refunds the falsely stolen cash to the account holder.

Counterfeit Ad Campaigns

Paid ads using stolen trademarks, images, and logos impersonate legitimate brands and lure victims to counterfeit stores on the open web. These ads are associated with fake business pages on social media, appear authentic, and feature heavily discounted products. If a victim clicks on an ad, they are directed to a fake website selling unauthorized goods.

Money Flipping Scam

Money Flipping

The threat actor promises a substantial payment to the victim in return for small amounts of cash. Once the victim transfers payment, the scammer ceases communication and disappears along with the money.

Card Cracking

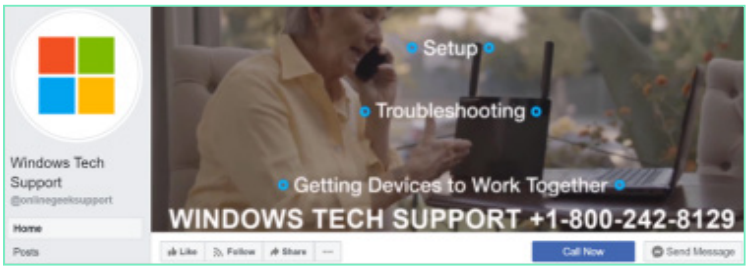
Similar to deposit fraud, a victim reports a credit card stolen and gives the threat actor their bank account or card information. The threat actor then withdraws funds and divides the cash.

Tech Support

Threat actors request monetary compensation or access to the victim's computer to fix a supposed issue. Contact is made under the pretense of solving a particular problem and impersonation is used to add legitimacy.

Fake Employment Opportunities

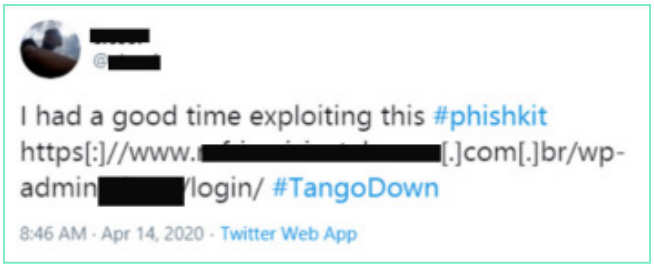
Threat actors impersonate fake companies regarding potential employment. During the bogus interview process, they request money for processing fees or personally identifiable information (PII) that can be used to financially harm the victim by other means.



Tech Support Scam

Cyber Threats

These threats on social media platforms consist of phishing and malware attacks. Phishing examples range from links or pages containing phishing information, to something as simple as general tips to running a campaign.



Phishing Information

Data Leaks

There are four types of sensitive data that are leaked on social media:

- Customer and employee PII
- Credentials such as usernames and passwords
- Sensitive documents including contracts and company projects
- Source code, which gives the threat actor access to internal software

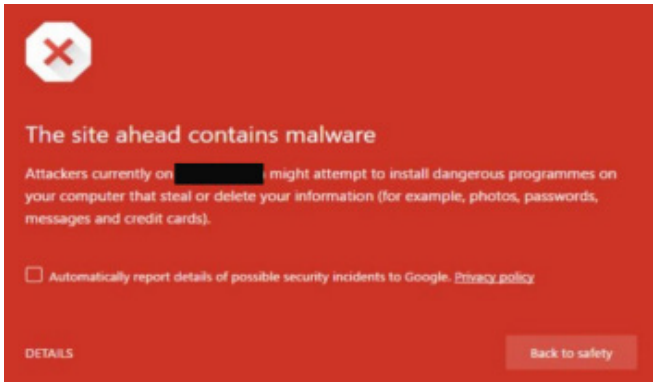
Leaked Source Code

Reputation Risks

An organization's reputation can be damaged if they are the victim of any social media threat type listed above. In addition, threat actors can post defamatory comments or make unauthorized associations with a business to draw unwanted, negative attention.

Protests, petitions, and boycotts also cause reputational damage, and risk physical harm to employees or customers. To successfully monitor for reputation risks, it is important to track any upcoming concerns or mentions related to your organization.

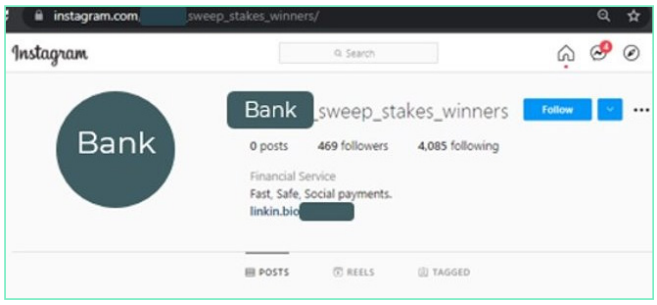
Malware can manifest as links in comments, posts, or direct messages. If installed, threat actors can gain access to the victim's computer and hold it, as well as account information, hostage.



Malware

Brand, Employee, and Executive Impersonation

Threat actors use impersonation to maximize effectiveness of scams across social networks. Impersonating high-ranking executives, employees, and recognizable brands aids in malicious efforts by adding familiarity and credibility. Common scams that use impersonation include fake giveaways and contests.



Brand Impersonation

Which Industries Are Targeted and Why

No organization is immune to social media threats, although some face a higher risk of attack than others. The following are industries commonly targeted by threat actors.

Financial Institutions

Among the most common threat types for financial institutions are leaked PII, documents, credentials, and source code. A source code leak can lead to a data breach and publicizing of proprietary information. The reputational damage associated with these threats can be severe and result in loss of brand trust as well as wavering investor confidence.

Phishing attacks and brand impersonation are also common threats to financial institutions. A successful phishing campaign can ruin a customer's finances and, depending on the organization's response to the attack, negatively impact future business, customer trust and overall public reputation.

Media and Entertainment

Threat types to media organizations are more specific to the industry and include tech support scams, employment scams, and leaked PII. Victims of tech support or employment scams may have their credentials stolen, credit card numbers leaked, or social security numbers compromised, which can lead to financial loss. Organizations have the potential to suffer massive indirect costs as a result of these scams due to customer distrust.

Healthcare

One of the threat types considered high risk for healthcare is tech support. These scams are particularly prevalent because they are easily created, modified, and mimicked. Tech support scams can result in stolen PII and credentials from patients and clients.

Leaked documents also have a devastating impact on healthcare providers due to the sensitive nature of information they interact with. Threat actors can leak documents to scam, blackmail, or even harm a customer.

Retail

Impersonation and counterfeit ad campaigns are the primary threat types targeting retail, with brands, employees, and C-suite executives at risk. These attacks are easy to set up using stolen intellectual property and are low cost to the threat actor. Impact can range from revenue loss through the decline of repeat and future sales, as well as brand damage.

Turning Social Media into Intelligence

Security teams must have processes in place that ensure the delivery of accurate, highfidelity intelligence to streamline response times and reduce the lifespan of threat workloads. To thoroughly gather the data to do this, they must look for threats spanning all social media platforms that apply to their organization. To accelerate the gathering and accurate curation of intelligence, enterprises should leverage a combination of machine processing and human analysis.

There are four components to turning social media data into actionable intelligence:

- Classify the threat
- Determine its severity
- Eliminate false positives
- Add context

Given the vast amount of data on social media, potential threats must be classified using advanced algorithms that identify targeted references while filtering out false positives. Techniques like fuzzy matching or customized criteria — such as relevant keywords or brand activity — are commonly employed to achieve this.

Expert analysts must also apply business context to the threats to assess the risk they pose. Without this context, legitimate threats may be overlooked and benign activity may be misinterpreted as malicious.

To ensure alignment and speed up mitigation, analysts must be well-versed not only in the organization's specifics and audience but also deeply attuned to its priorities and unique needs beyond just social media. Understanding the threat as it relates to a specific brand will ensure analysts can accurately determine relevancy and prioritize severity. Finally, the resulting intelligence must be enriched with context and tuned in response to any changing business needs before being actioned.

Taking Down Social Media Threats

Security teams must have multiple takedown options available to select the most appropriate response for each situation. Mitigation processes vary, and takedowns can be complex and challenging. To execute takedowns effectively, teams should build direct relationships with social media platforms, enabling swift action in high-risk scenarios.

Networks and Criteria

Financial scams remain widespread across major platforms such as X, Facebook, and Instagram. Each of these social networks offers built-in reporting tools within their platforms and user profiles. Additionally, X and Facebook provide dedicated channels for security teams to submit direct reports of malicious activity, enabling faster response and mitigation.

Mitigation criteria:

- Direct mentions of client in question with intent to commit financial fraud
- Posted login details
- Break in terms of service

Cyber threats are found on all major networks including YouTube and paste sites. Platforms aren't simply looking at what content is on the post, and any information relating directly or indirectly to the cyber threat reported needs to be submitted as evidence in order to successfully mitigate.

Mitigation criteria:

- Active links to malicious content that are abusive in nature
- Proof of past posted malicious content

Executive and corporate impersonation are utilized in many of the threat types seen on social media. These scams are found on all major platforms. There are many intricacies in filling out and submitting forms for impersonation, and reporting these types of threats includes direct contact with the platforms.

Mitigation criteria:

- Proof that the profile is not a parody account
- Proof that the name and photo of the person impersonated is present on the post
- Legitimate profile of the victim is optimal

Identifying and Mitigating Social Media Threats

As social media continues to evolve and expand, so do the tactics of threat actors exploiting these platforms. By staying informed, leveraging targeted intelligence, and adopting proactive mitigation strategies, security teams can effectively safeguard their organizations against emerging social media threats. This guide serves as a foundation, empowering you to navigate the complex social media landscape with confidence and resilience.

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

Copyright © Fortra, LLC and its group of companies. Fortra®, the Fortra® logos, and other identified marks are proprietary trademarks of Fortra, LLC.

(fta-pl-gd-0625-r3-vm)